TOO GOOD TO BE TRUE….

A Column on Consumer Issues by Attorney General Wayne Stenehjem's Consumer Protection and Antitrust Division

July 26, 2006

"Vishing: Voice Phishing"

Over the past several years, we have had to learn new terminology to keep up with our exploration on the Internet. Terms such as "spam," "phishing," and "pharming" have become common lingo for Internet users. Organizations such as the Federal Trade Commission and the North Dakota Attorney General's Consumer Protection and Antitrust Division have been making tremendous gains in educating computer users to the types of scams on the "information highway." As a result of these educational efforts, the con artists have come up with a new scam utilizing a new technology.

"Vishing," or voice phishing, uses Voice over Internet Protocol (VoIP) phones instead of a misdirected Web link to steal user information. Instead of asking the consumer to click on a web-link as is done in "phishing," the consumer is asked to call a phone number, usually a toll-free number. The problem with this is, the number isn't to a bank or credit card company, it is to a VoIP phone that can recognize telephone keystrokes. Because part of the scam is carried out offline, it goes undetected by many computer security systems.

Sometimes, the con artists don't even use an email-blast, they use a VoIP system to blanket the area with telephone calls. A recorded message tells the consumer that their credit card has been breached and to "call the following phone number immediately." The call return number is spoofed to appear as a regional telephone number of the financial institution the criminals are pretending to represent.

This is made easier by the VoIP. Internet telephone service allows computer users to quickly establish phone numbers, often without verification checks used by traditional telephone companies. Internet phone companies dole out numbers with a choice of area code, regardless of where in the country the user is located. The real VoIP number could be anywhere in the world.

When the consumer calls the number, a message is played stating "this is account verification, please enter your 16 digit account number." Some of these "vishing" scams are even asking for the valuable three-digit security code on the back of credit cards. If the information is given by the consumer, chances are pretty good that their credit card will be used to make unauthorized purchases.

"Vishing" con artists send out thousands of messages to email addresses believed to be located in a specific area, hoping to reach actual customers of a particular business. In many cases, consumers who receive the emails are not actual customers of the "business" and they delete the email. Unfortunately, there are consumers who do

business with the “company” and respond to the email with the requested account information.

If you receive an email or a phone call instructing you to call a telephone number, don’t use that number. Contact your credit card provider or bank directly with the telephone number you have used in the past. You should also be suspicious of any phone or email contact that does not use their first and surnames. NEVER provide private information based on an email request.

The Attorney General’s Consumer Protection Division investigates allegations of fraud in the marketplace. Investigators also mediate individual complaints against businesses. If you have a consumer problem or question, call the Consumer Protection Division at 328-3404, toll-free at 1-800-472-2600, or 1-800-366-6888 (w/TTY). This article and other consumer information is located on our website at www.ag.nd.gov.

* * * * *